AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions

Year: 2021 | Citations: 365 | Authors: Iqbal H. Sarker, Md. Hasan Furhad, Raza Nowrozy

---

Abstract

Artificial intelligence (AI) is one of the key technologies of the Fourth Industrial Revolution (or Industry 4.0), which can be used for the protection of Internet-connected systems from cyber threats, attacks, damage, or unauthorized access. To intelligently solve today's various cybersecurity issues, popular AI techniques involving machine learning and deep learning methods, the concept of natural language processing, knowledge representation and reasoning, as well as the concept of knowledge or rule-based expert systems modeling can be used. Based on these AI methods, in this paper, we present a comprehensive view on "AI-driven Cybersecurity" that can play an important role for intelligent cybersecurity services and management. The security intelligence modeling based on such AI methods can make the cybersecurity computing process automated and intelligent than the conventional security systems. We also highlight several research directions within the scope of our study, which can help researchers do future research in the area. Overall, this paper's ultimate objective is to serve as a reference point and guidelines for cybersecurity researchers as well as industry professionals in the area, especially from an intelligent computing or AI-based technical point of view.